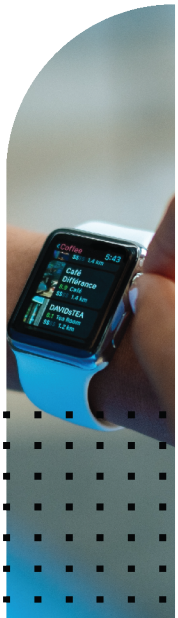
Release Notes

FortiManager 7.0.3



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 14, 2022
FortiManager 7.0.3 Release Notes
02-703-772393-20221214

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-02-02	Initial release.
2022-02-03	Updated FortiProxy information in Feature support on page 22.
2022-02-04	Updated FortiProxy on page 21.
2022-02-09	Added support for FortiOS 7.0.5 to FortiOS and FortiOS Carrier on page 19.
2022-02-10	Added 781118 to Known Issues on page 45.
2022-02-11	Updated FortiManager VM subscription license on page 7 and Appendix A - FortiGuard Distribution Servers (FDS) on page 52.
2022-02-15	Added information about support for FortiFirewall and FortiFirewallCarrier.
2022-02-15	Added FortiGate-7000E to FortiGate special branch models on page 28.
2022-02-23	Added special notice about SDN fabric connectors to Special Notices on page 10.
2022-03-07	Updated Supported models on page 7.
2022-03-15	Updated Resolved Issues on page 36 and Known Issues on page 45.
2022-03-17	Updated FortiGate special branch models on page 28. Updated Upgrade Information on page 15.
2022-03-23	Updated Special Notices on page 10.
2022-03-30	Updated Special Notices on page 10.
2022-04-07	Updated Special Notices on page 10.
2022-05-20	Updated Known Issues on page 45 and Resolved Issues on page 36.
2022-06-20	Updated Known Issues on page 45 and Special Notices on page 10.
2022-07-07	Updated Upgrade Information on page 15.
2022-10-28	Updated FortiProxy on page 21.
2022-11-16	Updated FortiSandbox on page 21.
2022-12-14	Updated Resolved Issues on page 36.

FortiManager 7.0.3 Release

This document provides information about FortiManager version 7.0.3 build 0254.

The recommended minimum screen resolution for the FortiManager GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

Supported models

FortiManager version 7.0.3 supports the following models:

FortiManager	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, and FMG-3900E.
FortiManager VM	FMG_DOCKER, FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see FortiManager VM firmware on page 15.

See also Appendix B - Default and maximum number of ADOMs supported on page 53.

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager7.0.3.

FortiManager uses port TCP/443 or TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the FortiManager 7.0 Ports Guide.

Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

FortiManager	FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, and FMG-3900E.
FortiManager VM	FMG_DOCKER, FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

Minimum system requirements

By default FortiManager VMs use the following system resource settings:

- 4 vCPU
- 8 GB RAM
- 500 GB disk space

Starting with FortiManager 7.0.0, RAM and CPU is capped at 50% for MEAs. (Use the `config system docker` command to view the setting.) If FortiManager has 8 CPUs and 16 GB RAM, then only 4 CPUs and 8 GB RAM are available to MEAs by default, and the 4 CPUs and 8 GB RAM are used for all enabled MEAs.

Some management extension applications have minimum system requirements that require you to increase system resources. The following table identifies the minimum requirements for each MEA as well as the recommended system resources to function well in a production environment.

MEA minimum system requirements apply only to the individual MEA and do not take into consideration any system requirements for resource-sensitive FortiManager features or multiple, enabled MEAs. If you are using multiple MEAs, you must increase the system resources to meet the cumulative need of each MEA.

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiAIOps	• 8 vCPU • 32 GB RAM • 500 GB disk storage	No change
FortiAuthenticator	• 4 vCPU • 8 GB RAM	No change
FortiPortal	• 4 vCPU • 8 GB RAM	No change
FortiSigConverter	• 4 vCPU • 8 GB RAM	No change

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiSOAR	• 4 vCPU • 8 GB RAM • 500 GB disk storage	• 16 vCPU • 64 GB RAM • No change for disk storage
Policy Analyzer	• 4 vCPU • 8 GB RAM	No change
SD-WAN Orchestrator	• 4 vCPU • 8 GB RAM	• 4 vCPU • 12 GB RAM
Universal Connector	• 1 GHZ vCPU • 2 GB RAM • 1 GB disk storage	No change
Wireless Manager (FortiWLM)	• 4 vCPU • 8 GB RAM	No change

*The numbers in the *Recommended system resources for production* column are a combination of the default system resource settings for FortiManager plus the minimum system requirements for the MEA.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.0.3.

FAP-831F not yet supported by AP Manager

The AP Manager module does not yet support the FAP-831F model.

Authorizing FortiGate with FortiClient EMS connected

Please follow the steps below when managing FortiClient EMS Connector's configuration via FortiManager:

1. Add a FortiGate device to FortiManager.
2. Create FortiClient EMS Connector's configuration on FortiManager.
3. Install the configuration onto the FortiGate device.

If the order of the steps is not followed, FortiClient EMS may not authorize the FortiGate device.

View Mode is disabled in policies when policy blocks are used

When policy blocks are added to a policy package, the *View Mode* option is no longer available, and policies in the table cannot be arranged by *Interface Pair View*. This occurs because policy blocks typically contain multiple policies using different incoming and outgoing interfaces, however, *View Mode* is still disabled even when policy blocks respect the interface pair.

FortiManager upgrades from 7.0.0

When upgrading from FortiManager 7.0.0, you must first upgrade to 7.0.1 before going to 7.0.2 and later. This is required to correct an issue that causes FortiManager to download unnecessary objects from FortiGuard. Please contact FortiManager support for more information if required.

SDN fabric connectors

According to the current design, SDN fabric connectors are installed on all FortiGates in an ADOM, even if the fabric connectors are not in use. See also bug ID 496870 in Known Issues on page 45.

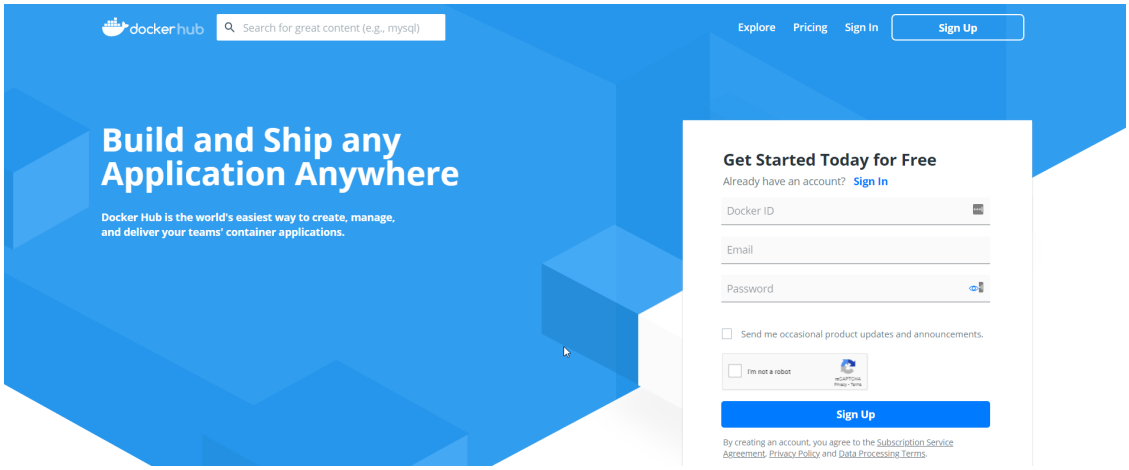
Workaround: Place FortiGates in another ADOM when you do not want to install SDN fabric connectors to the devices.

Fortinet verified publisher docker image

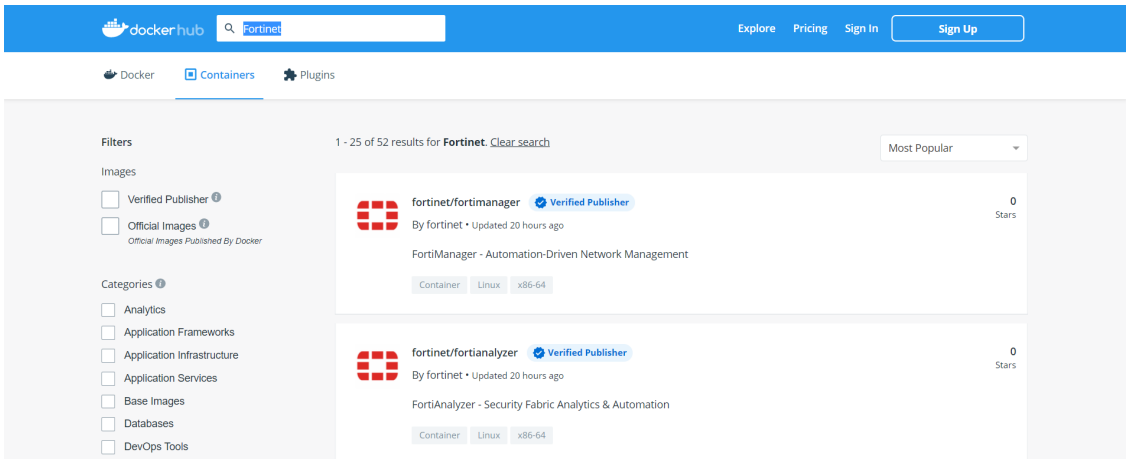
FortiManager 7.0.1 docker image is available for download from Fortinet's Verified Publisher public repository on dockerhub.

To download the FortiManager image from dockerhub:

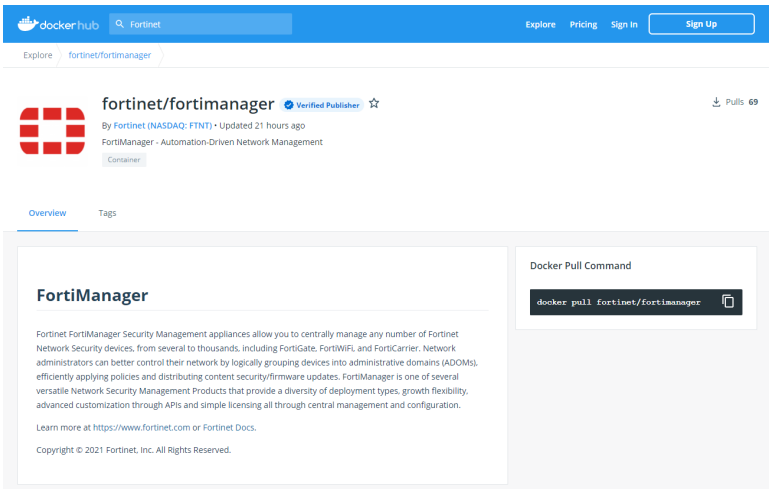
1. Go to dockerhub at https://hub.docker.com/.
   The dockerhub home page is displayed.



2. In the banner, click *Explore*.
3. In the search box, type *Fortinet*, and press *Enter*.
   The *fortinet/fortimanager* and *fortinet/fortianalyzer* options are displayed.



4. Click *fortinet/fortimanager*.
   The *fortinet/fortimanager* page is displayed, and two tabs are available: *Overview* and *Tags*. The *Overview* tab is selected by default.



5. On the *Overview* tab, copy the docker pull command, and use it to download the image.
   The CLI command from the *Overview* tab points to the latest available image. Use the *Tags* tab to access different versions when available.

Scheduling firmware upgrades for managed devices

Starting in FortiManager 7.0.0, firmware templates should be used to schedule firmware upgrades on managed FortiGates. Attempting firmware upgrade from the FortiManager GUI by using legacy methods may ignore the *schedule upgrade* option and result in FortiGates being upgraded immediately.

Modifying the interface status with the CLI

Starting in verion 7.0.1, the CLI to modify the interface status has been changed from `up`/`down` to `enable`/`disable`.

For example:

```
config system interface
   edit port2
      set status <enable/disable>
   next
end
```

SD-WAN with upgrade to 7.0

Due to design change with SD-WAN Template, upgrading to FortiManager 7.0 may be unable to maintain dynamic mappings for all SD-WAN interface members. Please reconfigure all the missing interface mappings after upgrade.

Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:
   ```
   xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
   ```
2. Confirm the setting is in effect by running `xenstore-ls`.
   ```
   ----------------------
   limits = ""
   pv-kernel-max-size = "33554432"
   pv-ramdisk-max-size = "536,870,912"
   boot-time = ""
   ---------------------------
   ```
3. Remove the pending files left in `/run/xen/pygrub`.

The ramdisk setting returns to the default value after rebooting.

Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol t1sv1
```

```
    end
```

Upgrade Information

You can upgrade to FortiManager 7.0.3 from the following versions:

- FortiManager 6.4.0 to 6.4.x
- FortiManager 7.0.1 to 7.0.x

If you are upgrading from FortiManager 7.0.0, upgrade to FortiManager 7.0.1, and then upgrade to 7.0.3. See also FortiManager upgrades from 7.0.0 on page 10.

For other upgrade paths and details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

This section contains the following topics:

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release by using the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrade process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in, go to *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Google Cloud Platform

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiManager VM installation.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `<product>_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `<product>_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Microsoft Hyper-V 2016 is supported.

Oracle Private Cloud

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.opc.zip`: Download the 64-bit package for a new FortiManager VM installation.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager Data Sheet available on the Fortinet web site. VM installation guides are available in the Fortinet Document Library.

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

Product Integration and Support

This section lists FortiManager 7.0.3 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

Supported software

FortiManager 7.0.3 supports the following software:

To confirm that a device model or firmware version is supported by the current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```

Always review the Release Notes of the supported platform firmware version before upgrading your device.

Web browsers

FortiManager 7.0.3 supports the following web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 96
- Google Chrome version 97

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS and FortiOS Carrier

The *FortiManager Release Notes* communicate support for FortiOS versions that are available at the time of the FortiManager 7.0.3 release. For additional information about other supported FortiOS versions, please refer to the FortiManager compatibility chart in the Fortinet Document Library.

See FortiManager compatibility with FortiOS.

FortiManager 7.0.3 supports the following versions of FortiOS and FortiOS Carrier:

- 7.0.0 to 7.0.5
- 6.4.0 to 6.4.8
- 6.2.0 to 6.2.10

FortiADC

FortiManager 7.0.3 supports the following versions of FortiADC:

- 6.2.0 and later
- 6.1.0 and later
- 6.0.0 and later

FortiAnalyzer

FortiManager 7.0.3 supports the following versions of FortiAnalyzer:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

FortiAuthenticator

FortiManager 7.0.3 supports the following versions of FortiAuthenticator:

- 6.4.0 and later
- 6.3.0 and later
- 6.2.0 and later

FortiCache

FortiManager 7.0.3 supports the following versions of FortiCache:

- 4.2.0 and later
- 4.1.0 and later
- 4.0.0 and later

FortiClient

FortiManager 7.0.3 supports the following versions of FortiClient:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.1 and later

FortiDDoS

FortiManager 7.0.3 supports the following versions of FortiDDoS:

- 6.2.0 and later
- 6.1.0 and later
- 6.0.0 and later

Limited support. For more information, see Feature support on page 22.

FortiDeceptor

FortiManager 7.0.3 supports the following versions of FortiDeceptor:

- 4.1 and later
- 4.0 and later
- 3.3 and later

FortiFirewall and FortiFirewallCarrier

FortiManager 7.0.3 supports the following versions of FortiFirewall and FortiFirewallCarrier:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

FortiMail

FortiManager 7.0.3 supports the following versions of FortiMail:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

FortiProxy

FortiManager 7.0.3 supports configuration management for the following versions of FortiProxy:

- 7.0.2

Configuration management support is identified as *Management Features* in these release notes. See Feature support on page 22.

FortiManager 7.0.3 supports logs from the following versions of FortiProxy:

- 7.0.0 to 7.0.5
- 2.0.0 to 2.0.5
- 1.2.0 to 1.2.13
- 1.1.0 to 1.1.6
- 1.0.0 to 1.0.7

FortiSandbox

FortiManager 7.0.3 supports the following versions of FortiSandbox:

- 4.2.0 and later
- 4.0.0 and 4.0.1
- 3.2.0 and later
- 3.1.0 and later

FortiSOAR

FortiManager 7.0.3 supports the following versions of FortiSOAR:

- 6.4.0 and later
- 6.0.0 and later

FortiSwitch ATCA

FortiManager 7.0.3 supports the following versions of FortiSwitch ATCA:

- 5.2.0 and later
- 5.0.0 and later
- 4.3.0 and later

FortiTester

FortiManager 7.0.3 supports the following versions of FortiTester:

- 7.0.0 and later
- 4.2.0 and later
- 4.1.0 and later

FortiWeb

FortiManager 7.0.3 supports the following versions of FortiWeb:

- 7.0.0 and later
- 6.4.0 and later
- 6.3.0 and later

Virtualization

FortiManager 7.0.3 supports the following virtualization software:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012, 2016, and 2019
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- Oracle Private Cloud
- VMware ESXi versions 5.0, 5.5, 6.0, 6.5 , 6.7, and 7.0

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiGate	✓	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓	✓
FortiADC		✓	✓		
FortiAnalyzer			✓	✓	✓

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiAuthenticator					✓
FortiCache			✓	✓	✓
FortiClient		✓		✓	✓
FortiDDoS			✓	✓	✓
FortiDeceptor		✓			
FortiFirewall	✓				✓
FortiFirewall Carrier	✓				✓
FortiMail		✓	✓	✓	✓
FortiProxy	✓	✓	✓	✓	✓
FortiSandbox		✓	✓	✓	✓
FortiSOAR		✓	✓		
FortiSwitch ATCA	✓				
FortiTester		✓			
FortiWeb		✓	✓	✓	✓
Syslog					✓

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiManager Administration Guide.*

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 7.0.3.

Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

FortiGate models

The following FortiGate models are released with FortiOS firmware. For information about supported FortiGate models on special branch releases of FortiOS firmware, see FortiGate special branch models on page 28.

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60EDSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate3960E, FortiGate-3980E **FortiGate 5000 Series**: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate DC**: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiWiFi**: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE **FortiGate VM**: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-ARM64-KVM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGateVM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM **FortiOS**: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGateRugged**: FortiGateRugged-60F, FortiGateRugged-60F-3G4G	7.0

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate DC:** FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiGate Hardware Low Encryption:** FortiGate-100D-LENC **FortiWiFi:** FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, **FortiGate VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGateRugged:** FortiGateRugged-60F, FortiGateRugged-60F-3G4G	6.4

Model	Firmware Version
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-GBL, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FG-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-400E-Bypass, FG-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000C, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7000F **FortiGate DC:** FortiGate-80C-DC, FortiGate-401E-DC, FortiGate-600C-DC, RortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC **FortiGate Hardware Low Encryption:** FortiGate-80C-LENC, FortiGate-100D-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC **FortiWiFi:** FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-POE, **FortiGate-VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager **FortiGate Rugged:** FortiGateRugged-30D, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-90D **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	6.2

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.0.3 supports these models on the identified FortiOS version and build number.

For information about supported FortiGate models released with FortiOS firmware, see FortiGate models on page 24.

FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	7.0	Build 291 and special branch 4334
FortiGate-3500F FortiGate-3501F	7.0	Build 294 and special branch 4344
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	7.0	Build 291 and special branch 4334
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	7.0	Build 291 and special branch 4334
FortiGate-4400F, FortiGate-4400F-DC FortiGate-4401F, FortiGate-4401F-DC	7.0	Build 291 and special branch 4334

FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	6.4.8	6165
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	6.4.8	6165
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	6.4.8	6165
FortiGate-80F-POE, FortiGate-81F-POE	6.4.7	5944
FortiWiFi-80F-2R FortiWiFi-81F-2R FortiWiFi-81F-2R-3G4G-POE FortiWiFi-81F-2R-POE	6.4.7	5944
FortiGate-3500F	6.4.6	5886
FortiGate-3501F	6.4.6	6132

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-4400F, FortiGate-4400F-DC FortiGate-4401F, FortiGate-4401F-DC	6.4.6	5868
FortiGate-6000F	6.4.6	1766
FortiGate-7000E, FortiGate-7000F	6.4.6	1766

FortiOS 6.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80D	6.2.10	5168
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	6.2.9	7197
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	6.2.9	7197
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	6.2.9	7197
FortiGate-4400F, FortiGate-4400F-DC	6.2.9	7197
FortiGate-4401F, FortiGate-4401F-DC	6.2.9	7197
FortiWiFi-80F-2R-3G4G-DSL FortiWiFi-81F-2R-3G4G-DSL	6.2.6	7219
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099

FortiCarrier models

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC**: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC	7.0

Model	Firmware Version
FortiCarrier-VM: FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen, FortiCarrier-ARM64-KVM	
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC **FortiCarrier 6K and 7K:** FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7000F, FortiCarrier-7121F, FortiCarrier-7121F-2 **FortiCarrier 6K and 7K DC:** FortiCarrier-6000F-DC, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC, FortiCarrier-7060E-8-DC, FortiCarrier-7121F-DC, FortiCarrier-7121F-2-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.2

FortiADC models

Model	Firmware Version
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F **FortiADC VM**: FortiADC-VM	6.2

Model	Firmware Version
FortiADC: FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F **FortiADC VM**: FortiADC-VM	6.0, 6.1

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E **FortiAnalyzer VM**: FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E **FortiAnalyzer VM:** FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4
FortiAnalyzer: FAZ-200D, FAZ-200F, FAZ-300D, FAZ-300F, FAZ-300G, FAZ-400E, FAZ-800F, FAZ-1000D, FAZ-1000E, FAZ-1000F, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3000G, FAZ-3500E, FAZ-3500F, FAZ-3500G, FAZ-3700F and FAZ-3900E. **FortiAnalyzer VM:** FortiAnalyzer-DOCKER, FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.2

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	6.2, 6,3, 6.4

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E **FortiCache VM:** FCH-KVM, FCH-VM64	4.1, 4.2
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E **FortiCache VM:** FCH-VM64	4.0

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F **FortiDDoS VM**: FortiDDoS-VM	6.0, 6.1, 6.2

FortiDeceptor models

Model	Firmware Version
FortiDeceptor: FDC-1000F, FDC-1000G **FortiDeceptor Rugged**: FDCR-100G **FortiDeceptor VM**: FDC-VM	4.1
FortiDeceptor: FDC-1000F, FDC-1000G **FortiDeceptor Rugged**: FDCR-100G **FortiDeceptor VM**: FDC-VM	4.0
FortiDeceptor: FDC-1000F, FDC-3000D **FortiDeceptor VM**: FDC-VM	3.3

FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.0.3 supports these models on the identified FortiFirewall firmware version and build number.

Model	Firmware Version	Firmware Build
FortiFirewall: FortiFirewall-3980E **FortiFirewall DC**: FortiFirewall-3980E-DC	6.2	1262
FortiFirewall: FortiFirewall-4200F	6.2.7	5141
FortiFirewall: FortiFirewall-4400F	6.2.7	5148

FortiFirewallCarrier models

The following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.0.3 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version	Firmware Build
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.2.7	5148

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E **FortiMail VM:** FML-VM	7.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E **FortiMail VM:** FML-VM	6.2, 6.4

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E **FortiProxy VM:** FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.0
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E **FortiProxy VM:** FortiProxy-KVM, FortiProxy-VM64	1.2, 2.0

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC **FortiSandbox-VM:** FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.0
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC	3.1, 3.2

Model	Firmware Version
FortiSandbox-VM: FortiSandbox-AWS, FSA-VM	

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FortiSOAR-VM	6.0, 6.4

FortiSwitch ATCA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5903C, FTCL-5913C	5.2
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B	5.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3

FortiTester models

Model	Firmware Version
FortiTester: FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.0
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.2
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.1

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E, FortiWeb-4000F **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.4, 7,0
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.3

Resolved Issues

The following issues have been fixed in 7.0.3. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
691540	Where Used should indicate that an AP is still in used in one or more FortiGate devices.
697444	SSID with MPSK may not pass verification during an install.
726287	Deleting Floor Map may return a blank popup with error.
750255	FortiManager should enable DFS channels on WTP profiles for FAP234F and FAP231F with region N.
750458	AP Manager should not send local-authentication for VAP with wpa-enterprise and Radius to managed FortiGate.
755675	FortiManager may remove radius configuration from VAP when using "security wpa3-enterprise".
757706	FortiManager might downgrade FortiAP with enforce firmware version.
763233	AP profile may not contain SSID when AP Manager is in central management mode.
772194	FortiManager should not install the setting, set security-redirect-url, without making any such change.

Device Manager

Bug ID	Description
673008	SD-WAN Rules order changes to the default when creating a rule and moving it to the top.
699893	SD-WAN's priority-members is missing from CLI configuration page.
709214	System template should allow source interface to be selected when specify is activated as interface-select-method.
712578	FortiManager does not allow WiFi SSID with special characters.
726721	Unable to add multiple DNS domain names in provisioning template.

Bug ID	Description
729301	A managed FortiGate with assigned CLI template remains in "modified" state following a successful device configure installation.
733379	FortiManager cannot edit global level configuration when management VDOM is not in the current ADOM.
735360	When editing a device group, search results do not show the device if VDOM name is matched by search keyword first.
740428	Device Manager is unable to display and download conflict URL filter firewall objects during import.
740893	Secondary IP may be purged when setting a description to VLAN interface.
742543	NTP server system template advance options may not be saved.
744628	After exported system template, importing the same configuration via CLI may fail.
744973	FortiManager GUI throws an error when switching from Policy & Objects to Device Manager.
747955	There may be performance issue when onboarding new SD-WAN devices.
748240	When FortiAnalyzer is managed via FortiManager, new devices that are registered to FortiManager should be synchronization under the corresponding ADOM on FortiAnalyzer.
749823	Named Address Static Route with SD-WAN cannot be selected on FortiManager.
749923	SD-WAN logs cannot be saved for some devices when sdwan-monitor-history is set as enabled.
750303	Under *System* > *Interface*, the data shown on this page may be incomplete.
750838	FortiManager may fail to import device list from another FortiManager due to the meta field containing prefix "_meta_".
752666	Provisioning System Templates page may stuck when an entry contains forward slash character.
753258	FortiManager may be unable to show SD-WAN monitor data when the rtmmond daemon is stuck.
754228	If a device group has been added as a group member, it should reside only as a group member and not as a root device group.
754465	FortiManager should also count promoted hidden devices.
754952	Deleting an interface referenced in the dashboard stops FortiManager auto-update.
755388	SD-WAN Monitor may not display any device when a device does not have any port monitor data.
755519	Zero-touch provisioning with script installation may fail due to duplicated snmp-index.
759905	When creating a device zone, device mapping may not be created when the zone is mapped to a normalized interface with the 'map as zone only' option.
760099	When creating EMAC VLAN from *Device Manager*, FortiManager should show VLAN ID field.

Bug ID	Description
760132	*Device Manager* may not be able to delete FortiGate-7000E HA cluster members.
760579	FortiManager may not be able to install meta field variable used in SD-WAN profile to multiple FortiGate devices.
762082	When creating a Static Route, FortiManager may take a few seconds to display available "Named Address".
762365	When creating a static route, FortiManager may not be able to assign interface.
762650	FortiManager is sending commands which do not exist in FortiGates; issue happens only on 80/81F and 60F.
763797	Installation fails due to configuring forward-error-correction on FortiGate's interfaces.
767647	Map view may not show device status properly.
769303	FortiManager may not be able to delete Firmware Template with special characters.
770829	FortiManager may raise error when using the meta field SD-WAN template neighbor.
773147	Installation fails due to the unexpected system interface config changes for "pvc" related settings.

FortiSwitch Manager

Bug ID	Description
748200	FortiSwitch monitor may show incorrect interface status for QSFP port.
756609	There may be issues to rename FortiSwitch template if it is imported using the import configuration option.
760538	Adding a new FortiSwitch template for FortiSwitch-108F may fail due to invalid data source for dsl-profile.
764258	FortiManager should not update trunk-member value as it is controlled by FortiGate.
770471	Importing FortiSwitch may fail due to NAC segment.

Global ADOM

Bug ID	Description
660852	FortiManager should not save invalid default value for ssl-ssh-profile in global database.
725763	Automatic install to ADOM devices may fail from Global ADOM.

Bug ID	Description
741942	FortiManager should show clear error message for duplicated object assigned from Global ADOM.
755201	Policy package list is empty after created an admin and specific the access to Global ADOM.
758903	After upgraded FortiManager, all Global policies are still assigned as before but with Status "Pending changes".
760417	Internet Services may not be displayed in Global Database ADOM.
760804	FortiManager may return an error when adding address object to global policy.

Others

Bug ID	Description
605560	Flag is_model and linked_to_model are not working for add model device with JSON API.
622448	FortiManager should support the FortiClient EMS Fabric Connector.
732116	Setting of "FortiCloud Single Sign-On" is always displayed on login.
738639	Users should be able to obtain status of the fgfm reclain-dev-tunnel via API call.
740523	Retrieve task may fail due to autoupdate file already been deleted by fgfm.
744197	If an VDOM is created and then get the VDOM information from JSON API, the VDOM mode may be shown as NULL.
750419	Execution of integrity check may remove dynamic mappings.
756555	There should be a dignose command to reset or remove rating statistics database.
763669	FortiManager Pay-As-You-Go should support connect to FortiCare via proxy.
764674	Map should use the region defined by the coordinates in System Settings' Advanced Settings or the FortiManager's time zone.
766105	FortiManager may not be able to upgrade ADOM from 6.2 to 6.4 due to cdb crash.

Policy and Objects

Bug ID	Description
748467	FortiManager does not have the same profiles as on FortiGate with explicit proxy policy.
713886	FortiManagre returns an error, "method failure", when setting a shaping profile in normalized interface using per device mapping.

Bug ID	Description
717031	FortiManager doesn't update the "Hit Count" number.
718223	Hyperscale firewall EIF shall not be enabled when IP pool with CGN overload configuration is used in a policy.
719104	FortiManager may not be able to select Internet Service group members when creating Internet Service group.
721253	FortiManager may not import all the roles and address groups from ClearPass.
726328	SSL-SSH profile may display incorrect options when using SSL Certificate Inspection.
729179	FortiManager may not be able to add Geography type address when interface mapping is enabled.
732199	FortiManager displays the group ID instead of display name with NSX-T Connector.
733602	FortiManager should support multiple GCP projects within a single SDN connector.
736115	FortiManager may not be able to create Web Forwarding Server Group.
737062	FortiManager may unset shaping profile with per-device mapping.
738114	FortiManager should return a proper message for error such as "get install scripts error (st=4,err=-8)".
738475	Special characters within policy's comment causes all policies missing on GUI.
744049	Proxy policy does not accept configuration with both ipv4 and ipv6 address objects.
744766	FortiManager may not be able to retrieve IP address for group with NSX-T v3.1.2.
744934	FortiManager may try to install undesirable changes to FortiGate-5001E, FortiGate-5001E1, and FortiGate-5001D.
745884	FortiManager GUI may not response when triggering policy package install wizard under Policy & Objects.
747537	Where Used should show the correct object references for newly cloned objects.
747558	FortiManager filters should work for HitCounters, First Session, and Last session.
748222	Cloning of a policy package is greyed out for admin users with restricted access to particular policy packager folder.
748235	Filtering by hit count may not work for policies.
748246	"Where Used" may result an empty top left frame for policy packages.
748498	There may be issue with Transparent Web Proxy when using interface pair view.
748556	FortiManager should not allow users to create Explicit proxy FTP with pool name.
749576	FortiManager may try to install hidden synproxy parameters for DOS policy to FortiGate.
750539	If FortiGate allows selecting LogMeIn app using specific filter override, FortiManager should also allow it.
750882	User may not be able to save changes in SSL/SSH inspection profile from GUI.

Bug ID	Description
751137	There may be install performance issue when there is a huge number of dynamic mappings and there are many FortiAP or FortiSwitch devices.
751710	Editing a global user FSSO object's dynamic mapping is not possible.
752777	FortiManager should be able to manage valid authentication rules containing "User-Agent" proxy address.
752822	FortiManager may not response when adding a firewall address or group to a policy and changing the policy comment at the same time.
754225	Policy package status is out of sync without changes.
755072	Type mac address object without any mac addresses listed causes addresses table does not show entries.
755233	FortiManager should install the agent successfully for FSSO via FortiGate.
755252	Plus "+" sign should be added for SMS phone number when two-factor FortiToken Cloud is enabled.
755348	FortiManager should support more than one thousand traffic shapers.
757164	FortiManager database contains parameter webfilter-searchengine-Baidu-gb2312 that does not exist on FortiGate.
758021	After upgrading FortiManager, editing a policy with locking policy package duplicates the policy.
758526	FortiManager should be able to delete many per-device mappings quickly.
758534	Address objects which are MAC Address type may not be lost after upgrade.
758809	When policy package in policy-based NGFW mode, FortiManager may still set action to accept even when the policy is specified as deny.
760436	FortiManager may not be able to enable reputable website for SSL/SSH Inspection profile.
760869	Deleted objects may remain referenced in firewall policy.
761072	FortiManager may prompt "Cannot modify" error when using right-click menu to add object to policy.
765793	Adding custom signature with '_vdom-name' should not prevent pushing changes to numerous devices.
765812	Hyperscale policy packages do not show log server until you get into a policy.
767317	Policy Hit Count may not be updated for Read-Only admin.
768353	Commit action is taking too much time and it makes the FMG slow.
769997	Selection for user SAML as member under the user group may not take effect.
770678	Changing Action from Accept to Deny should ignore all UTM profiles within the firewall policy.
770700	FortiManager may install changes to a different device than the FortiGate selected.

Revision History

Bug ID	Description
618305	FortiManager changes configuration system csf settings.
657424	FortiManager may disable the "l2forward" and "stpforward" settings on virtual switch interface when installing policy package.
660525	When installing from FortiManager, it may unset comment, organization, and subnet-name during install.
691240	FortiManager should not unset the value *forward-error-correction* with certain FortiGate platforms.
700495	FortiManager 6.2 ADOM may be sending set synproxy to FortiGate-1801F.
722604	After removed a member of user group that is used only in XAUTH, FortiManager is not deleting the unused local user on FortiGate.
740858	GCP project name must be set during install.
748350	Explicit proxy FTP ssl-ssh-profile application-list may not be installed.
748462	FortiManager should not set the HA interface IP under the central-management on FortiGate when the master unit fails.
750637	FortiGate-5001E, FortiGate-5001E1, and FortiGate-5001D may be mistakenly set to support switch-profile.
751771	Users may not be able to create hardware switch interface from FortiManager.
751776	Renaming IPSec Phase1 that is a member of a zone causes all zone related rules to be re-created.
752764	Install wizard may purge key-string for OSPF interface authentication.
753724	After imported and edited policy with NAT46, the subsequent install may fail due to NAT setting.
754081	Application Control signatures belong to Industrial Category are removed from FortiGate in split mode during policy install.
755059	After disabled NAT on hyperscale policy, there may be installation failure on unset action.
756508	FortiManager may unset chassis ID causing HA cluster lost.
757716	There may be install issue with Web Filter's "config ftgd-wf" which does not exist on NGFW policy mode on FortiGate.
761968	FortiManager may not be able to install resource limits to FortiGate.
764497	FortiManager should not create a new wildcard FQDN object while renaming it.
767824	FortiManager may unexpectedly delete custom signature when installing policy package.

Script

Bug ID	Description
384139	Filter does not work on device group.
654700	Users need to open "View Script Execution History" to see that TCL script fails.
740938	Direct CLI script may fail when it contains an 'exec' command.
757156	When running CLI script remotely on 100+ firewalls, partial configuration is retrieved and it may cause routing to be removed from device database.
762611	Policy package status should not go out-of-sync when an automated script is triggered.

Services

Bug ID	Description
718256	FMG-VM64-AWSOnDemand may not retrieve the proper license when it is behind a proxy.
746680	FortiGate cannot update to latest patch due to image list not updated.
753871	FortiClient packages should not continue to be received once the service for that firmware version has been disabled.

System Settings

Bug ID	Description
687992	Backup that includes IPSec VPN cannot be restored.
553488	TACACS is unable to assign multiple ADOMs to admins.
634220	Event logs should record changes related to CLI Template.
640670	If a user specified ADOMs including global ADOM, workflow approval may not be able to find the same user.
697328	When trying to change Chassis ADOM status to disable, FortiManager may prompt "not defined" error.
706303	Template assignment or save may not generate clear Event logs.
734422	The "svc sys" daemon may have high memory usage when API is used to upgrade FortiGate devices.
737142	FortiManager should support using the special character "@" in SNMP community name.

Bug ID	Description
738395	FortiManager tasks' time used should not be increased by timezone.
745288	Meta field variable does not works in System Templates for interface widget when action is set as DHCP Server.
745333	Remote authentication servers should not be synchronized among HA members.
745365	Event log may be truncated when the log contains many address objects.
745449	Link color is not clear to see when hovering over or selecting the link.
746568	FortiManager may continuously changing NTP synchronization server.
747181	Idle timeout may not work for SSO user.
748237	Users may not be able to disable ADOM via GUI or CLI.
748860	User may not be able to upgrade Backup ADOM.
751069	User may not be able to disable ADOM after upgrade.
758975	FortiManager may not be able to upgrade ADOM from v6.4 to v7.0 due to change with replacement message.
760427	FortiManager is not able to upload MIB files without any error message.
762708	LDAP may stuck for twenty seconds if LDAP is not responding.

VPN Manager

Bug ID	Description
735417	FortiManager may purge mac-addr-check-rule when installing to FortiGate.
748488	Cloned VPN Phase1 interface may have several different parameters than the original interface.
750227	Removing a spoke or hub from VPN community may result in partial configuration removal.
757734	FortiManager may unset peer if "peertype" is not set as "peer".

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
770575	FortiManager 7.0.3 is no longer vulnerable to the following CVE Reference: • CVE-2022-22300

Known Issues

The following issues have been identified in 7.0.3. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
708100	AP Manager cannot show Channels when 160 MHz channel width is set.
749820	*AP Manager* > *SSID* > *Advanced Options* may not list objects under the settings "address-group".
770234	5GHz DFS channels on AP Profile were not supported for FAP U231F.
772213	FortiManager may try to delete default *wtp 11ac-only profile* on FortiWiFi-60F causing install to fail.
781561	User may not be able to access AP Manager with custom read only admin profile.
785471	FortiManager was deleting wireless-controller wtp and the objects referenced by wtp during the first installation after the upgrade.

Device Manager

Bug ID	Description
545239	After added FortiAnalzyer fabric ADOM to FortiManager, Device Manager's log status, Log Rate, or Device Storage column cannot get data from FortiAnalyzer.
587404	FortiManager sets incorrect captive-portal-port value when installing v6.0 PolicyPackage to v6.2 devices.
651560	SD-WAN monitor may stuck loading when admin user belongs to device group.
677836	The Client Address Range setting should allow users to configure assign-IPs from firewall address or group.
704106	Certificate Enrollment fails using SCEP on Microsoft server with sub-ca certificate chains.
705212	When editing device in HA cluster, admin password change is not applied to secondary unit.
725334	Importing policy package shows ngfw-mode policy-based with the inspection-mode set to proxy.

Bug ID	Description
729413	FortiManager is missing peer options with dial up user configuration with VPN IPSec Phase 1.
743102	*Device & Groups* > *VPN Phase1/Phase2* does not show the proposal column when using FGT-VM type "FGVMIB".
748578	Retrieve FortiGate configuration may fail due to FSSO connector.
751427	Provisioning Template with empty name cannot be deleted or edited.
752443	Vertical scroll bar is missing in SD-WAN configuration.
759255	User may not be able to click on the check box to import configuration with 6.2 ADOM.
759708	The provisioning template 's status on Summary Dashboard always displays "Modified".
763907	Certificates CN information may be invalid when FortiGate is registered by Zero-Touch-Provisioning.
764369	FortiManager tries to install Security Fabric trusted list to all downstream FGs when a new one is added.
764841	FortiManager is unable to use secondary IP as source IP in DNS database.
765762	FortiManager is unable to install the *Switch controller* > *VLAN interface* configuration during the ZTP process.
767185	Unable to create route map rule using 'match-interface' when using the BGP Templates under the Provisioning Templates.
770567	When a device uses IPsec Tunnel Provisioning template with enable value for aggregate member, FortiManager may create a new system interface with the same name which is not expected behavior.
770600	Comma between IP address and subnet causes saving problem on Prefix List Rule under BGP Templates.
773336	FortiToken provision button is greyed out in Device Manager while it is enabled on FortiGate with the same token.
776605	Editing provisioning CLI template without any modification may cause device status changed to *Modified*.
779836	FortiManager cannot install TCP-connect using Random port for SD-WAN.
779900	Administrative user GUI-dashboard information should be deleted upon VDOM deletion.
780833	FortiManager cannot use space to set location under SNMP configuration.
783517	Input-Device under *CLI Configuration* > *System* > *SD-WAN* > *Service* displays loading forever.
791117	Unable to create simultaneous static routes with named address objects.
791274	When optional meta fields are being used users cannot edit the devices.
793941	Unable to install VPN psk with special characters through CLI template.

Bug ID	Description
794368	Removing the objects from Device Level DB did not delete the objects' reference from ADOM Level DB.
795913	Error Probe Failure has been observed when adding FortiAnalyzer to FortiManager.
799259	Duplicate CSF groups for 7.0 FortiGates (7.0.2+) due to syntax returning upstream-ip instead of upstream.

Global ADOM

Bug ID	Description
691562	Threat feeds global objects are not installed to destination ADOM when using the assign all object option.
740942	"srcintf" selector in Traffic Shaping Header or Footer Policy may not work in Global ADOM.
743734	Cannot remove objects from Global Database.
752328	Global database may be locked when viewing Workflow Session Diff.
795327	When adding an ADOM to Global Database, the message "Double global assignment exists" keeps showing up.

Others

Bug ID	Description
703585	FortiManager may return 'Connection aborted' error with JSON API request.
707911	FortiManager should be able to assign VLAN interface to FortiExtender.
729175	FortiManager should highlight device consisting of specific IP address under *Fabric View*.
747716	JSON API does not return gateway for IPSec route.
774872	FortiManager should support more than 88 characters for password when backing up all settings.
775574	There is a Criteria Latency field which is different between FGT & FMG when creating the manual interface option for SDWAN rules.
776342	System NPU values may be different between FortiManager and FortiGate-1801F.
776413	FortiManager Lock/commit operation is very slow when FortiManager HA is enabled.
781642	FortiManager displays "failed to copy BRANCH_BGP_Recommended" error when performing the "check adom-integrity" test.

Bug ID	Description
781831	FortiManager should be able to retrieve EMS tags using hostname of FortiClient EMS Server if its able to resolve the hostname.
783226	*Fabric View* may keep loading.
786281	During the installation, FortiManager displays Policy Consistency Check failure without any clear reason.
792887	Verification fail for default dnsfilter profile due to wrongly install "set category 0".

Policy & Objects

Bug ID	Description
701750	The App Control set to Monitor in FortiManager causes the App to disappear from FortiGate.
713692	Web Filter Profile install may fail when using pre-defined URL filter.
725427	Policy package install skips the policy where destination interface is set as SD-WAN zone and policy is IPSEC policy.
731037	There may be File Filter file type mismatch between FortiGate and FortiManager.
751767	Export to excel when filters are applied for a policy package does not work.
758494	Searching members inside an address group does not work.
758680	Unable to complete the Cisco pxGrid fabric connector's configuration on FortiManager.
767255	FortiManager fails to install the custom signature because it is too long.
770210	Where used may not reporting used objects properly.
770256	FortiManager displays error when using "push to install" for objects utilized by policy blocks.
771165	Removing the objects from Device Level DB did not delete the object's reference from ADOM Level DB.
771941	FortiManager is unable to import or create virtual server with real servers using the same IP but different "http-host".
773249	FortiManager may not display the correct number of firewall address objects while adding the objects to DoS policy.
773333	For User, the configurations for two-factor-authentication and two-factor-notification should not lead to installation failure.
773403	FortiManager may now differentiate between the ISDB objects "Predefined Internet Services" and "IP Reputation Database".
774058	Rule list order may not be saved under File Filter Profile.

Bug ID	Description
774111	FortiManager does not support Dynamic firewall address with sub-type Switch Controller NAC Policy TAG.
774435	Right-click menu to add object may return an error: "cgn-resource-quote:out of range".
775128	Unable to create more than 20 SAML users in policy package object.
776361	Policy lookup may not work if the managed devices are in Transparent mode.
777017	FortiManager purges the "arrp-profile" when installing the v6.2 policy packages to v6.4 FortiGates.
777554	There may be slowness when using Find Duplicate Objects with Merge tools.
777879	Copy fail error due to external-resource used in webfilter profile.
778111	Removing the objects from Device Level DB did not delete the object's reference from ADOM Level DB.
779853	When creating a Central DNAT policy in FortiManager, more services may not be added to policy with error: can't assign to property "from" on NaN: not an object.
779947	Address group changes for per-device mapping does not apply to FortiGate when Address group is used in policy route.
779965	Users may not be able to export firewall Header and Footer policies to Excel.
781118	6.4 version ADOM policy package failed to enable policy NAT from GUI
781118	ADOM version 6.4 policy package failed to enable policy NAT from GUI.
782435	Moving a policy by dragging may not work properly.
783899	There may not be empty lines in "IPS Signature and Filters".
785341	Consolidated policy NAT is always disabled on the GUI.
786684	Installation fails because the virtual-wan-link did not exist.
786740	FortiManager displays Install failure due to adding "g-" prefix to the external-resource objects.
789957	Created time doesn't indicate AM or PM on the *Tools* > *Find Unused Policies*.
792980	Installation fails when trying to install SAML user configuration.
797091	"Synchronize Firewall Addresses" under the FortiClient EMS Connector does not automatically create and synchronize addresses for all EMS tags.
801876	Installation failed due to "Copy global shared objects" failure.
805783	After the 6.0 ADOM upgrade, installing the same v6.0 policy package got "unset webfilter-profile" in wanopt proxy policy.

Revision History

Bug ID	Description
496870	Fabric SDN connector is installed on FortiGate, even if it is not in use.
729148	Install fails when new transparent mode VDOM is added directly via FortiGate CLI and imported into FortiManager.
774115	After upgrade, install may fail for FSSO password when private-data-encryption is enabled.
775577	AutoUpdate may purge firewall shaping-profile.

Script

Bug ID	Description
766019	Failed to run the Post-Run CLI Template due to the "datasrc invalid" error.
767577	Installing a script to device database fails if switch-interface member contains VXLAN interface.
780604	When creating a new phase1 interface, dpd=on-idle settings may not be saved.
787113	TCL scripts fails to run if the admin's password is longer than 36 characters.
793407	Installation fails if one of the BGP network prefix entry is a supernet.

Services

Bug ID	Description
798979	FortiManager cannot download the latest IPS DB.

System Settings

Bug ID	Description
728972	"fmDeviceEntSupportState" OID returns incorrect value for some devices.
752916	FortiManager should be able to set desired permissions for *Extender Manager* in administrator profile settings.
753690	SNMPv3 security option configuration has discrepancy between GUI and CLI.

Bug ID	Description
762663	FortiManager should have the CA Identifier as configurable for SCEP server request.
768636	Password cannot be longer than 63 characters for configuration auto backup.
768682	Setting a Cluster ID for a model HA cluster results in an invalid group ID under config system HA.
775091	Two factor authentication fails when special characters are used in CN.
777726	FortiManager may not generate event logs for meta field changes.
778405	Script Groups should be copied with their members when cloning an ADOM.
782345	FortiManager may not be able to upgrade ADOM from 6.2 to 6.4: err=-2,Policy ippool (ippool6) name cannot be empty.
783066	The number of FortiGate devices registered is in the upper limit of the license count may causes HA becomes asynchronized.
787588	Webfiltering HTTPS 8888 is not working after FMG upgraded from 6.4.7 to 7.0.4.
790409	idle_timeout under admin's setting is not converted properly after performing the upgrade.

VPN Manager

Bug ID	Description
615890	IPSec VPN Authusergrp option "Inherit from Policy" is missing when setting xauthtype as auto server.
699759	When installing a policy package, per device mapped objects used in SSL VPN cannot be installed.
773710	When editing an existing SSL VPN settings, the Banned-cipher and cipersuite may be keep changing.
774040	Keyboard-layout configuration in VPN SSL web portal predefined RDP bookmark generates incorrect commands.
779498	VPN monitor may not display correct information when FortiManager is in advanced ADOM mode.
780154	Policy package should be pushed to VPN hubs without error, "interface IP is 0".

Appendix A - FortiGuard Distribution Servers (FDS)

In order for FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as an FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the following items:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default, and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through port 443.

FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform:

Platform	Update Service	Query Service
FortiGate	✓	✓
FortiCarrier	✓	✓
FortiClient	✓	
FortiDeceptor	✓	✓
FortiMail	✓	✓
FortiProxy	✓	✓
FortiSandbox	✓	✓
FortiTester	✓	
FortiWeb	✓	

Appendix B - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiManager hardware models and virtual machines.

Hardware models

FortiManager supports a default number of ADOMs based on hardware model.

Some hardware models support an ADOM subscription license. When you purchase an ADOM subscription license, you increase the number of supported ADOMs. For example, you can purchase an ADOM subscription license for the FMG-3000G series, which allows you to use up to a maximum of 8000 ADOMs.

Other hardware models do not support the ADOM subscription license. For hardware models that do not support the ADOM subscription license, the default and maximum number of ADOMs is the same.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
200G Series	30		30
300F Series	100		100
400G Series	150		150
1000F Series	1000		1000
2000E Series	1200		1200
3000G Series	4000	✓	8000
3700G Series	10,000	✓	12,000

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the FortiManager Data Sheet.

Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Licenses are non-stackable. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the FortiManager Data Sheet.

www.fortinet.com